на базі модулів сплітерів-репітерів. Загальнодержавний міжвідомчий науково-технічний збірник. Конструювання, виробництво та експлуатація сільськогосподарських машин. Кропівницький: ЦНТУ, 2021. Вип. 51. С. 195-202

4. Смірнов В.В., Смірнова Н.В., Практична реалізація безпровідної мережі «Easy Net Everywhere». M 58 International security studios: managerial, technical, legal, environmental, informative and psychological aspects. International collective monograph. Volume I. NMBU, Research and Education. 2024. - 700 p. Oslo, Kingdom of Norway - 2024. С.665 - 697.

УДК 005.95/.96:(004.4+331.5)

ЦИФРОВІ ТЕХНОЛОГІЇ В УПРАВЛІННІ: АКТУАЛЬНІ ТЕНДЕНЦІЇ ТА ВИКЛИКИ В УМОВАХ ВОЄННОГО СТАНУ

О. Сторожук, канд. екон. наук, доцент
О. Сокуренко, аспірант
Центральноукраїнський національний технічний університет

Ринковий успіх у бізнесі залежить від здатності працівників підприємств володіти актуальними знаннями, навичками та компетенціями. Це потребує постійного навчання та розвитку персоналу. Зміни в бізнес-середовищі відбуваються дуже швидко, тому працівники повинні бути гнучкими та адаптованими до нових умов. Розвиток інформаційних технологій робить можливим більш широке використання віддаленої роботи, нових форм співпраці в колективі та автоматизації бізнес-процесів. Крім того, роки повномасштабної російсько-української війни показали, як пропаганда та дезінформація використовують різні технології та канали, щоб маніпулювати громадською думкою, спричиняти розкол у суспільстві та підривати довіру до офіційних джерел. Тому уміння використовувати цифрові технології в управлінні стає головною умовою вирішення багатьох проблем економічного розвитку як окремого підприємства, так і національної економіки загалом, що підкреслює актуальність обраної теми дослідження.

У часи воєнного стану цифрові технології відіграють вирішальну роль, забезпечуючи комунікацію, координацію та інформаційну підтримку в системі управління підприємством. Проте, виступаючи благом, цифрові технології також є джерелом багатьох викликів. До прикладу, зростає використання месенджерів, соціальних мереж та інших онлайн-платформ для координації дій та обміну інформацією, що дає змогу швидко реагувати на ситуацію та підтримувати зв’язок навіть у складних умовах. Водночас, в умовах воєнного стану суттєво збільшуються ризики кібератак. Так, 12 грудня 2023 року масштабна кібератака на «Київстар», одного з найбільших мобільних операторів України, позбавила зв’язку 24,4 мільйона абонентів [4]. Послуги оператора були недоступні протягом кількох днів, що спричинило паніку та колосальні незручності для населення й бізнесу. У січні 2024 року кіберзлочинцями був атакований дата-центр «Парковий», де обслуговуються десятки державних структур. Внаслідок атаки частково вийшли з ладу сервіси компанії «Нафтогаз України», АТ «Укрпошта», АТ «Укрзалізниця» [1]. Ці події спричинили перебої в роботі критично важливих державних сервісів та принесли фінансові збитки для компаній та держави.

Бойові дії несуть постійну загрозу пошкодження інфраструктури, включаючи електропостачання, інтернет-з’єднання та інші комунікації, що ускладнює доступ до цифрових бізнес-ресурсів, роботу в онлайн-режимі, а також підтримку контактів з клієнтами та постачальниками. Так, лише протягом весни 2024 року масовані удари росії зруйнували Трипільську ТЕС у Київській області, теплоелектростанцію «Зміївська» - у Харківській та дуже пошкодили Сумську ТЕЦ [2].

В умовах нестабільності зростає ризик втрати або знищення важливих даних, тому підприємства повинні забезпечити у своїй роботі резервне копіювання та належне зберігання критично важливої інформації, а також розробити плани на випадок непередбачуваних обставин. Слід зауважити, що в Україні діє Закон «Про захист персональних даних», який, як і

в Європейському Союзі, спрямований на захист прав і свобод громадян від неправомірного використання їхніх персональних даних. Цей закон визначає норми щодо збору, зберігання, обробки та передачі персональних даних, а також передбачає відповідальність за їх незаконне використання. На жаль, українське законодавство щодо захисту персональних даних не встановлює чітких територіальних обмежень. Крім того, в Україні відсутні жорсткі санкції за порушення вимог захисту персональних даних.

Воєнний стан суттєво впливає на різні аспекти суспільного та економічного життя, в тому числі спонукає велику кількість підприємств перейти на віддалену роботу, що викликає труднощі з точки зору організації процесів, підтримки продуктивності та комунікації між працівниками [5]. Необхідно забезпечити надійні інструменти для віддаленої роботи, що вимагає додаткових затрат фінансових ресурсів.

Цифрові технології використовуються для управління ланцюжками постачання, але під час воєнного стану виникають перешкоди в логістиці, транспортуванні та комунікації з постачальниками, що впливає на доступність матеріалів і ресурсів для бізнесу.

Таким чином, змушені констатувати, що в умовах воєнного стану управління цифровими технологіями на підприємствах стає все більш складним завданням. Напрями подолання таких викликів можуть полягати у наступному:

- створення плану дій на випадок надзвичайних ситуацій, який містить декілька підпланів: резервного копіювання та відновлення; підплан кібербезпеки; підплан комунікацій;
- посилення захисту інформації через механізми використання надійних паролів, встановлення оновлень програмного забезпечення, використання антивірусного програмного забезпечення, тотальне навчання співробітників кібербезпеці;
- забезпечення безупинної роботи ІТ-інфраструктури за допомогою використання резервних джерел живлення, резервних каналів зв’язку та хмарних технологій.

Такі заходи, звісно, є затратним і вимагають спеціалізованих знань, але вони виправдовують себе, оскільки користі від них більше. Крім того, безпекові інфраструктури є важливими для захисту від кіберзагроз підприємств та організацій та надання їм стійкості в умовах кризи [3], найжахливішою з яких, за наслідками, є війна.

Резюмуючи, відзначимо, що цифрові технології відіграють все більшу роль у діяльності та соціально-економічному розвиткові підприємства. Вони використовуються для навчання персоналу, посилення командної роботи, налагодження ефективних виробничих комунікацій. Щоб бути успішними та конкурентоспроможними, сучасним підприємствам важливо навчити своїх працівників володіти навичками впевненого, критичного і відповідального використання цифрових технологій, а також постійно удосконалювати свою роботу із подолання викликів, які генерує зовнішнє середовище діяльності, особливо в умовах воєнного стану.

Список літератури

1. Водяний А. Хакери атакували датацентр «Парковий»: постраждали система «Шлях», Нафтогаз, Укрпошта, УЗ. ULR: https://biz.liga.net/ua/all/it/novosti/masshtabna-kiberataka-systema-shliakh-i-servisy-naftohazu-tymchasovo-vyishly-z-ladu (дата звернення 30.04.2024)

2. Карбунар Н. Нічний обстріл енергетичних об’єктів: рятувальники продовжують ліквідовувати наслідки. ULR: https://glavcom.ua/country/incidents/nichnij-obstril-enerhetichnikh-objektiv-rjatuvalniki-prodovzhujut-likvidovuvati-naslidki--998155.html (дата звернення 30.04.2024)

3. Немченко Т., Коваленко В. Менеджмент організацій ІТ-сектору в кризових умовах розвитку економіки. Розвиток обліку, аудиту та оподаткування в умовах інноваційної трансформації соціально-економічних систем : Матеріали XI Міжнародної науково-практичної конференції, 30 листопада 2023 р. Кропивницький: ЦНТУ, 2023. С. 321-323. ULR: https://eti.edu.ua/images/files/zbirnuk2023.pdf.

4. Тарасовський Ю. «Київстар» назвав офіційну причину масового збою мережі. ULR: https://forbes.ua/news/kiivstar-nazvav-ofitsiynu-prichinu-masovogo-zboyu-merezhi-12122023-17830 (дата звернення 30.04.2024).

5. Marta Kopytko, Nataliia Grabar, Oksana Storozhuk, Yuliia Borutska, Tetiana Doroshenko. Influence of Negative Factors of War: Economic, Legal, Regional and Environmental Aspects. IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.6, May 2022. P. 13-18.